3. If the order of a group is divisible by p, a prime, there is at least one substitution of order p.
4. The substitutions of a group that omit a given letter form a group.

Cauchy, the Founder of Group Theory.

Terminology.—Cauchy's work on groups is found in his *Exercises d'analyse et de physique mathematique* published in 1844, and in the series of articles published in the Paris *Comptes Rendus* in 1845–1846.[1] Cauchy defines permutation and substitution in the same way, but uses the latter term almost entirely. He uses several devices to denote a substitution, the most common being (x, y, z, u, v, w) where each letter is replaced by the one which follows it and the last by the first. He defines this as a cyclic substitution. In the article written in 1815[2] he defines the degree of a substitution as the first power of the substitution that reduces to identity, but later he also defines order in this way and uses the word order rather than degree in his subsequent work. He uses both the term unity and identical substitution. A transposition is defined and the terms similar, regular, inverse and permutable substitutions are found with their present day significance. A group he calls a "system of conjugate substitutions," which may be transitive or intransitive. A transitive imprimitive group is "transitive complex." The order of a system of conjugate substitutions is the number of substitutions that it contains. The term "divisor indicatif" is also found for the order of a group. Cauchy frequently transfers his definition of order to the theory of equations and speaks of the number of equal values a rational function can assume when the variables are permuted in every possible way. The number of distinct values of such a function is the index. In the early article the order of operation is from left to right, but in all his later work he reverses the order and operates from right to left.

The Memoir of 1815.—In the paper published in 1815 the one theorem which is of special interest is that the number of distinct values of a non-symmetric function of degree n cannot be less than the largest prime that divides n, without becoming equal to 2. This theorem is proved. He states the special cases, that if the degree of a function is a prime number greater than 2, the number of distinct values cannot be less than the degree; and that if the degree is 6 the number of distinct values cannot be less than 6. He makes special reference to the functions belonging to (1) the intransitive group of degree 6 and order 36; (2) the transitive imprimitive group of degree 6 and order 72; (3) the intransitive group of degree 6 and order 48; (4) and the symmetric group of degree 5 considered as an intransitive group of degree 6. The functions are as follows:

(1) $a_1a_2a_3 + 2a_4a_5a_6$,

(2) $a_1a_2a_3 + a_4a_5a_6$,

(3) $a_1a_2a_3a_4 + a_5a_6$,

(4) $a_1a_2a_3a_4a_5 + a_6$.

The Memoir of 1844.—In the memoir published in 1844 in his *Exercices d'Analyse* there is much more of importance. The first theorem proved is that

[1] *Œuvres de A. Cauchy*, First series, vols. 9 and 10.
[2] *Journal de l'Ecole polytechnique*, 10 (1815), p. 1.

every substitution similar to a given substitution P is the product of three factors, the extremes of which are the inverse of each other and the middle term of which is P. Conversely, every product of three factors, the first and last of which are the inverse of each other, is similar to the middle term P. An important formula developed is for the number of substitutions similar to a given substitution. If ω is the number required, n the total number of letters and P the given substitution, composed of f cycles of order a, g cycles of order b, h cycles of order c, etc., and r the number of letters fixed in P, then

$$\omega = \frac{n!}{(f!)(g!)(h!)\cdots(r!)a^f b^g c^h \cdots}.$$

Among other theorems that he proves in this article are the following:

1. If P is a substitution of order i, h any number and θ the highest common factor of h and i, then P^h is of order i/θ.

2. If P is a substitution of order i, the substitutions among the powers of P that are of order i are the powers of P whose indices are prime to i. These substitutions are likewise similar to P, and hence the number of substitutions similar to P among the powers of P are in number equal to the number of numbers less than i and prime to it.

3. Let P be any substitution, regular or irregular; let i be its order and p any prime factor of i. Then a value for i can always be found such that P^i is a substitution of order p.

4. A substitution and its inverse are always similar.

5. The powers of a cycle constitute the totality of substitutions that transform the given cycle into itself.

6. The order of a system of conjugate substitutions is divisible by the order of each substitution.

7. Two permutable substitutions with no common power but identity, together generate a system of conjugate substitutions whose order is the product of the orders of the two substitutions.

8. If $1, P_1, P_2, \cdots P_{a-1}$ and $1, Q_1, Q_2, \cdots Q_{b-1}$ are two groups, one of order a and the other of order b, which are permutable and have no common terms but identity, then the group generated by these groups is of order ab.

9. The converse of (8).

10. If P and Q are two substitutions, one of order a and the other of order b, and if the two series $Q, PQ, P^2Q, \cdots P^{a-1}Q$ and $Q, QP, QP^2, \cdots QP^{a-1}$ are made up of the same terms in the same or different order, then the cyclic group generated by P is permutable with the cyclic group generated by Q.

A most important element in establishing Cauchy's claim as the founder of group theory is the proof which he gives of the fundamental theorem that if m is the order of a group and p any prime which divides m, there is at least one substitution of order p. Galois had stated the theorem but had not proved it. Its importance is due to the fact that it is the first step toward Sylow's theorem which appeared nearly thirty years later. In this memoir there are a number of specific groups mentioned although no enumeration of groups of special degrees is attempted. The substitutions of several groups are written out. Among them are (1) the octic, (2) the four-group, (3) the holomorph of the cyclic group of order five, (4) the intransitive group of degree 6 and order 9 and (5) the intransitive group of degree 6 and order 16. In addition to these groups the substitutions of which are given, several other groups are mentioned, among them (1) the holomorph of order 42, (2) the group of degree 7 and order 21, (3) the holomorph of the cyclic group of order 9.

There is also mentioned a group of degree 9 and order 27, generated by the two substitutions

$$P \equiv x_0x_3x_6 \cdot x_1x_4x_7 \cdot x_2x_5x_8 \quad \text{and} \quad Q \equiv x_1x_2x_4x_5x_7 \cdot x_3x_6.$$

This is obviously impossible but a little study of his method reveals that he should have used $Q \equiv x_1x_3x_4x_5x_7x_8 \cdot x_3x_6$, and that in order to get the order of the group he has incorrectly applied the theorems he was announcing and illustrating. The order of the group should be 18. The two theorems which he was illustrating may be stated as follows:

1. If P is a substitution on n letters, $P = x_0x_1x_2 \cdots x_{n-1}$, and if r is any number prime to n and if Q is a substitution derived from P by replacing each letter by another whose subscript is r times its own, then for any values of h and k

$$Q^kP^h = P^{r^kh}Q^k.$$

2. If in the above theorem we take v any divisor of n, distinct from unity, and let R be any substitution that replaces any letter x_l by the letter with the subscript $l + v$, then Q^kR^h generates a group of order vi, where i is the smallest value of k that satisfies the congruence $r^k \equiv i \pmod{n}$.

Since in the present instance r is 2, i must be 6. The order of the group is then $vi = 3 \cdot 6 = 18$, whereas Cauchy seems to take $i = 9$ and derives the order of the group $vi = 3 \cdot 9 = 27$.

The Memoirs of 1845–1846.—Some of the material in the memoirs[1] published in the *Comptes Rendus* had already appeared in the *Exercices*, but is treated more extensively here. There is much, however, in the later articles that is not touched in the *Exercices*. It is in the later memoirs that he first defines what he means by a system of conjugate substitutions. The definition is as follows:

I shall call derived substitutions all that can arise from the given substitutions by multiplying them one or more times by each other or by themselves; and the given substitutions together with all the derived substitutions form what I shall call a system of conjugate substitutions.

Then follow the general theorems:

1. If i is the order of a substitution P and a, b, c, $\cdots$ are the prime factors of i, then the substitution P and its powers form a group generated by the substitutions $P^{i/a}$, $P^{i/b}$, $P^{i/c} \ldots$.

2. If $P, Q, R, S, \cdots$ are the substitutions that leave a given function Ω invariant, they form a group whose order is the number of equal values of Ω when the variables are permuted in every possible way.

3. The order of a transitive group of degree n is n times the order of the subgroup that leaves one letter fixed.

4. If Ω is a transitive function on n letters, if m is the index of the corresponding transitive group under the symmetric group of degree n, then m will likewise be the index of the subgroup that leaves one letter fixed under the symmetric group of degree $n - 1$.

Intransitive Groups.—The general subject which Cauchy treats next is that of intransitive groups. He implicitly divides intransitive groups into two classes. The first class includes those in which the systems are independent, that is, in our terminology, those in which the systems of transitivity are united by direct product. The second class includes those in which the systems are dependent, that is, those in which the systems are united by some sort of iso-

[1] *Œuvres de A. Cauchy*, First series, volumes 9 and 10.

morphism. The concept of isomorphism is however only implied. He states first that an intransitive group is formed by the combination in some way of transitive constituents. He then develops some interesting formulas for the order of intransitive groups. If the systems are independent, then the order M is the direct product of $A, B, C, \cdots$ the orders of the transitive constituents and the index will be $n!/ABC \cdots$ where n is the total number of letters. This same formula holds also when the systems are not independent if $A, B, C \cdots$ are defined in a special way. These definitions are as follows:

Let A be the order of the first transitive constituent;
Let B be the number of substitutions involving letters in the second system without involving any of the first;
Let C be the number of substitutions involving letters in the third system, without involving any of the first or second, and so on.

With these definitions of $A, B, C, D \cdots$ the order of the intransitive group is $M = ABC \cdots$.

Imprimitive Groups.—Cauchy next turns to imprimitive groups. Here he confines himself almost entirely to the consideration of those imprimitive groups which are simply transitive and which have for the subgroup that leaves one letter fixed the direct product of the transitive constituents. In regard to this particular type of imprimitive groups, he gives several theorems which are of interest, even though he does not touch upon the broader and more general principles.

If in a simply transitive group the subgroup that leaves one letter fixed is an intransitive group formed by the direct product of its transitive constituents, the group is imprimitive. He considers the special cases $a > n/2$, $a < n/2$, $a = n/2$ in which a, the number of letters in the largest transitive constituent and n is the degree of the group.

The only theorems which he enunciates that apply to imprimitive groups in general are:

1. The number of letters in the systems of imprimitivity must be a divisor of the degree.
2. If A is the number of substitutions that permute the variables within the systems and K the number of ways the k systems can be permuted, then the order of the group is KA^k.

Symmetric Groups.—Cauchy then considers briefly symmetric groups. One theorem which he states with its corollaries is as follows:

If a transitive group of degree n has a symmetric subgroup of degree a, where $a > n/2$, then the group is symmetric on n letters.

For $n > 2$, a transitive group of degree n is symmetric if it contains a symmetric subgroup of degree $n - 1$.

If $n > 3$, a transitive group of degree n is symmetric if it contains a symmetric subgroup of degree $n - 2$. The special case $n = 4$ is excepted; for the octic group, belonging to the function $\Omega = xy + zu$ is symmetric on two letters, yet not symmetric on all four.

If $n > 4$, a transitive group of degree n is symmetric if it contains a symmetric subgroup of degree $n - 3$. The case $n = 6$ is excluded. A group requiring this exception is the imprimitive group of degree 6 and order 72 which contains the symmetric group of order 6.

If $n > 5$, a transitive group of degree n is symmetric if it contains a symmetric subgroup of degree $n - 4$. If $n = 6$ or $n = 8$, this does not hold. Cauchy gives as examples of the case $n = 6$ the imprimitive groups of degree 6 and orders 72 and 48.

Some Implied Theorems.—One of the most important and interesting parts of Cauchy's work on group theory is that in which he develops some complicated formulas from which we may easily deduce the theorem that the average number of letters in the substitutions of a transitive group is $n - 1$. Cauchy himself does not enunciate the theorem, although he brings the proof to the point where only the final statement is necessary to complete it. The formula for the case where the group is simply transitive is as follows:

$M = 2H_{n-1} + 3H_{n-2} + \cdots + (n-2)H_2 + n$ where M is the order of the group, n its degree and H_{n-r} the number of substitution involving $n - r$ letters.

Further development of these formulas leads to the two conclusions:

1. If G is l-fold transitive of degree n, the number of substitutions involving $n - l + 1$ letters is equal to or greater than $n(n-1)\cdots(n-l+2)/(n-l)\,l!$;

2. If G is simply transitive, of degree n, the number of substitutions involving n letters is equal to or greater than $n - 1$.

We find here the assertion that if in an l-fold transitive group $l + 1$ letters are left fixed, all are left fixed. That this is false is demonstrated by considering the imprimitive group of degree 6 and order 72. It is simply transitive and hence $l = 1$; but $l + 1 = 2$ letters may be left fixed without all being so.

The theorem that the order of the holomorph of a cyclic group is the product of the orders of the cyclic group and its group of isomorphisms is found implicitly in Cauchy. He gives two theorems relative to this point.

1. Let $P = x_0x_1x_2\cdots x_{n-1}$ be a substitution of order n. Let r be a primitive root of the modulus n, and I the smallest of the indices of unity belonging to the base r. Then let Q be the substitution that replaces x_l by x_{rl}. The order of Q will be I and the order of the group will be nI.

This I is nothing else than the order of the group of isomorphisms of the cyclic group. If n is a power of a prime p, then $I = n(1 - 1/p)$. When n is a prime then $I = n - 1$.

2. With the same hypothesis as in (1), P^a and Q^b, where a and b are divisors of n and I respectively, generate a group of order nI/ab.

Enumeration of Orders.—Cauchy was the first to attempt an enumeration of the possible orders of groups. This he did with a fair degree of accuracy up to and including the sixth degree. The enumeration including degree 5 is correct and complete, but several errors occur in the enumeration of those of degree 6. For instance, 150 is given as the index of a group of degree 6 under the symmetric group, although factorial six is not a multiple of 150.

Cauchy goes back to his original distinction between imprimitive groups with heads which are direct products and those with heads formed by isomorphisms. He gives as the possible orders of groups of degree 6 with heads the direct products of the transitive constituents, 72, 48, 24, 18, 16, and 8. The last two numbers are clearly impossible for there is no transitive group of degree 6 and order 8 or 16. The orders of the groups possible when the head is formed with isomorphisms are given as 6, 12, 4, while there is no imprimitive group of degree 6 and order 4. According to his classification there should also be included in this last enumeration 24 and 18. A complete omission occurs in the list of imprimitive groups since the groups of order 36 with two systems of imprimitivity are not mentioned. Otherwise the enumeration through degree 6 is correct and complete.

Errors of Cauchy.—The errors in Cauchy's work on group theory may be divided into two classes. The first and smaller class includes a number of serious errors in logic. The second class includes a large number of minor errors, some typographical, others arising through careless statement. All of the serious errors found have been noted in this paper with the exception of one to which attention has already been called.[1] He states an erroneous theorem on imprimitive groups in the following form.

If G_1 is a subgroup composed of all the substitutions that omit a given letter in a simply transitive group then G is imprimitive unless all the transitive constituents of G_1 are of the same degree.

Conclusion.—In conclusion we may say that the foundation period in the history of group theory includes the time from Lagrange to Cauchy inclusive; that at the beginning of this period group theory was a means to an end and not an end in itself. Lagrange and Ruffini thought of substitution groups only in so far as they led to practical results in the theory of equations. Galois, while broadening and deepening the application to the theory of equations may be considered as taking the initial step toward abstract group theory. In Cauchy while a group is still spoken of as the substitutions that leave a given function invariant, and the order of a group is still thought of as the number of equal values which the function can assume when the variables are permuted in every possible way, nevertheless quite as often a group is a system of conjugate substitutions and its relation to any function is entirely ignored.

In Cauchy's work it is to be noted that use is made of all the concepts originated by the earlier writers in substitution theory except those of Galois, a number of which would have proved powerful instruments in his hands, notably the idea of the invariant subgroup of which he makes no explicit use.

Because of the important theorems Cauchy proved, because of the break which he made in separating the theory of substitutions from the theory of equations and because of the importance that he attached to the theory itself, he deserves the credit as the founder of group theory.

HISTORY OF THE EXPONENETIAL AND LOGARITHMIC CONCEPTS.

By FLORIAN CAJORI, Colorado College.

V. Generalizations and Refinements Effected During the Nineteenth Century.

GRAPHIC REPRESENTATION.

The time of Wessel and Argand has been chosen as the beginning of a new epoch in our history, not because Wessel and Argand made any noteworthy advance in exponential and logarithmic theory, but because the graphic repre-

[1] See G. A. Miller in *Bibliotheca Mathematica* (1910), series 3, vol. 10, p. 321.

sentation of imaginaries for which the names of Wessel[1] and Argand[2] preëminently stand, led mathematicians gradually to recognize the *reality* of imaginaries and to feel the need of a more general and a more consequential development of the algebra of imaginaries. The graphic representation of imaginaries had engaged the attention of the Englishman, John Wallis, in the seventeenth century[3] and of the German W. J. G. Karsten in the eighteenth century. Wallis proposed different schemes, none of which satisfactorily visualized vector addition. As previously shown in this history, Karsten concentrated his effort upon the graphic representation of imaginary logarithms, rather than on imaginary numbers in general. In view of these facts the graphic representation due to Wessel and Argand, which was finally adopted by the rank and file of mathematicians through the commanding authority of C. F. Gauss,[4] was a real advance.

The Wessel-Argand diagram does not offer an obvious means of displaying the infinitely many-valued logarithms of a number. Half a century passed before a generalization of this diagram was effected for the display of all the logarithms. For the first half of the nineteenth century there existed no diagram which could take rank with that of the circular and hyperbolic arcs, invented by Karsten in the eighteenth century.

A necessary generalization of the Wessel-Argand diagram was effected by Bernhard Riemann through the surfaces now called "Riemann's surfaces." One purpose of these surfaces was the visualization of the different values of functions of complex variables. The logarithmic function was simply one of several elementary functions to which Riemann's idea applied. Karsten's scheme serves only for the logarithmic function and is therefore less general. Riemann's idea was outlined in his inaugural dissertation, in 1851, at Göttingen, in a paper bearing the title, *Grundlagen für eine allgemeine Theorie der Funktionen einer veränderlichen complexen Grösse.*[5] The reader will picture to himself two planes, one representing the complex numbers z, the other the complex values w, where w is an n-valued function of z. To each point of the z-plane correspond n points of the w plane. It is a purpose of Riemann's scheme to create a geometric representation which avoids the multiplicity of values of a many-valued function and enables one to treat the function as if it were uniform. For this purpose he assumes the w plane to be made up of n sheets or leaves, which together represent the values of w. To each point in one sheet corresponds only one of w; to the n points lying one below the other correspond the n different values of w

[1] *Essai sur la représentation analytique de la direction*, par Caspar Wessel, Copenhague, 1897. Translation of Wessel's memoir in *K. Danske Videnskabernes Selskabs Skrifter, Femte Del. Kjobenhavn*, 1799.

[2] *Essai sur une manière de representer les quantités imaginaires dans les constructions géométriques*, Paris, 1806. An English translation, with historical notes, was brought out by A. S. Hardy, (Van Nostrand) New York, 1881.

[3] G. Eneström, *Bibliotheca mathematica*, 3d S., Vol. 7, 1906–'07, pp. 263–269; *Encyclopédie d. scien. mathématiques*, 1908, T. I., Vol. 1, 5, p. 339, note 51; F. Cajori, *Am. Math. Monthly*, Vol. XIX, 1912, pp. 167–171.

[4] See C. F. Gauss, *Werke*, Bd. II, Göttingen, 1876, p. 95.

[5] B. Riemann, *Math. Werke*, 2. Auflage, Leipzig, 1892, pp. 1–43. See particularly p. 41.

which are gotten from one value of z. If for a certain value of z several values of w become equal to each other, the sheets are supposed to be connected with each other, forming a *branch-point*. For the purpose of exhibiting the continuous passage of one value of w into another, so-called *branch-cuts* are made, which are lines drawn between any two branch-points or from a branch-point to infinity. These branch-cuts are supposed to break the conection, so that there is no passage across them from one side of a sheet to the other side of the same sheet, but they establish a connection between one side of a sheet and the opposite side of some other sheet. Which particular sheets should be connected, depends, of course, upon the properties of the function. These *branch-cuts* and the connections along the cross-cuts between different sheets establish one continuous surface. Riemann makes some brief statements concerning the logarithmic function, but makes no drawing to illustrate the surface to which it gives rise. Applying Riemann's general scheme to the function $w = \log z$, we see that to the z-plane there corresponds a w-surface of infinitely many sheets with all the sheets hanging together at 0 and ∞ and with a branch-cut drawn from 0 to ∞.

Special attention to the graphic representation of the infinitely many values of the general power u^v, where $u = a(\cos\alpha + i \sin\alpha)$ and $v = x + iy$, was given by John Warren[1] of Jesus College, Cambridge, and thirty-one years later by H. Durège[2] of the university of Prag. Durège refers to the work of Warren and reëstablishes the latter's result that the points in a plane representing the values of one and the same power all lie upon a logarithmic spiral and are so distributed that the radius vectors of two successive points include the constant angle $2\pi x$. Durège proceeds to a more elaborate study of the wonderful spirals and their vectors.

Somewhat similar studies which culminated in a new graphic representation of the infinitely many logarithms of a complex number—a representation that has found wide acceptance in texts on the theory of functions of complex variables and is often preferred to the visualization by Riemann's surfaces—was given in 1871 by G. Holzmüller of Magdeburg in a paper, *Ueber die logarithmische Abbildung und die aus ihr entspringenden orthogonalen Curvensysteme.* Holzmüller[3] takes $Z = \log z$ and shows that, to each infinitely long strip of area of the Z-plane, drawn parallel to the x-axis, and of width 2π, there corresponds the entire z-plane; that to each strip drawn parallel to the y-axis there corresponds in the Z-plane a circular ring of definite width, which must, however, be taken as wound about itself an infinite number of times. To each point of the Z-plane corresponds only one point of the z-plane; to each point of the z-plane corresponds an infinite number of points of the Z-plane, all of which lie on a line parallel to the y-axis and appear at intervals of 2π. Thus Holzmüller pictures the geometric signi-

[1] J. Warren published two articles in the *Philosophical Transactions* for the year 1829, London, pp. 241 and 339.

[2] H. Durège, in *Zeitsch. f. Math. u. Physik*, Leipzig, Vol. 5, 1860, p. 345.

[3] *Zeitschr. f. Math. u. Phys.*, Leipzig, Vol. 16, 1871, pp. 269–289.

cance of the many-valuedness of the logarithm and the periodicity of the exponential function. He acknowledges suggestions received from a lecture by Schwarz of Zürich. Holzmüller connects these results with the Riemann surfaces, and proceeds to elaborate some of the wonderful properties of the logarithmic spiral and to show the connection of this with the Ptolemaic stereographic projection and loxodromic lines.

The use of the logarithmic spiral in the graphic representation of complex numbers and their logarithms to any base, real or complex, upon the Wessel-Argand plane, is explained by Irving Stringham and M. W. Haskell in papers which we discuss more fully under the classification of logarithmic systems.

[The next instalment will treat the general power and logarithm.]

CERTAIN THEOREMS IN THE THEORY OF QUADRATIC RESIDUES.

By D. N. LEHMER, University of California.

The definition of a quadratic residue is usually given as follows: *If an integer X can be found to satisfy the congruence,*

$$X^2 \equiv D(\text{mod } m)$$

where D is relatively prime to m, then D is said to be a quadratic residue of m. The restriction that D shall be relatively prime to m simplifies many results. There are theories, however, in which this restriction serves to cloud the results and in this paper we will not impose it. We proceed, first of all, to determine the number of residues for a given integer m, using the enlarged definition.

We take first of all the case where the modulus m is a power of an odd prime p. In the first place there will arise $\frac{1}{2}\varphi(p^a)$ distinct residues from the squaring of the numbers k, which are less than p^a, and prime to p, $p^a - k$ and k giving the same residues. Consider next the numbers kp, where k is prime to p. If two such numbers when squared give the same residue, we have:

$$k^2p^2 \equiv k_1^2p^2(\text{mod } p^a),$$

whence,

$$k_1^2 \equiv k_1^2(\text{mod } p^{a-2})$$

or

$$k \equiv \pm k_1(\text{mod } p^{a-2}).$$

Give now k the $\varphi(p^{a-2})$ values less than p^{a-2} and prime to p. The resulting squares furnish $\frac{1}{2}\varphi(p^{a-2})$ distinct residues. In the same way the numbers kp^2 where k is prime to p furnish $\frac{1}{2}\varphi(p^{a-4})$ distinct residues which also are different from those obtained from kp obtained above. Proceeding in this way we obtain for the total number of distinct residues:

$$\tfrac{1}{2}[\varphi(p^a) + \varphi(p^{a-2}) + \varphi(p^{a-4}) + \varphi(p^{a-6}) + \cdots] + 1$$

the unit being added for the residue zero.

For α even, the resulting formula is:

$$\frac{p^{\alpha+1}-p}{2(p+1)}+1 \quad (p \text{ an odd prime}).$$

For α odd:

$$\frac{p^{\alpha+1}-1}{2(p+1)}+1.$$

For m a power of 2, the result is somewhat different. There are $2^{\alpha-3}$ distinct residues resulting from the squares of the odd numbers. This is due to the congruence, $(2^{\alpha-2}-k)^2 \equiv (2^{\alpha-2}+k)^2 (\text{mod } 2^\alpha)$. There are $2^{\alpha-5}$ residues arising from the squares of the numbers $2k$ where k is odd. This comes from the congruence, $(2^{\alpha-3}-2k)^2 \equiv (2^{\alpha-3}+2k)^2 (\text{mod } 2^\alpha)$. Similarly there are $2^{\alpha-7}$ distinct residues arising from the squares of the numbers 2^2k where k is odd, and in general there are $2^{\alpha-(2\kappa+3)}$ residues arising from the squares of the odd multiples of 2^κ. Thus in case of α odd we have the series $2^{\alpha-3}+2^{\alpha-5}+2^{\alpha-7}+\cdots$, which terminates with 1, the last term resulting from odd multiples of 2 where $\lambda = (\alpha-3)/2$. There remain besides two residues; one resulting from 2^λ where $\lambda = (\alpha-1)/2$, and one from 2^λ where $\lambda = (\alpha+1)/2$. This last is seen to be zero, modulus 2, owing to the congruence,

$$(2^{\alpha+1/2} \cdot k)^2 \equiv 2^{\alpha+1} \cdot k^2 \equiv 0 (\text{mod } 2^\alpha).$$

For α odd therefore the formula is $(2^{\alpha-1}+5)/3$. For α even the result is $(2^{-3}+2^{\alpha-5}+2^{\alpha-7}+2)+2$; that is $(2^{\alpha-1}+4)/3$.

As illustrations of the results, the number of residues of the number $81 = 3^4$, is $(3^5-3)/2 \cdot 4+1$ or 31. The actual residues are: 0, 1, 4, 7, 9, 10, 13, 16, 19, 22, 25, 28, 31, 34, 36, 37, 40, 43, 36, 39, 52, 55, 58, 61, 63, 64, 67, 70, 73, 76, 79.

For the number $27 = 3^3$ the number is $(3^4-1)/2 \cdot 4+1$ or 11. The actual residues are: 0, 1, 4, 7, 9, 10, 13, 16, 21, 25.

For the number $32 = 2^5$ the formula gives $(2^4+5)/3 = 7$. The residues are: 0, 1, 4, 9, 16, 17, 25.

For the number $64 = 2^6$ we have $(2+4)/3 = 12$. The residues are: 0, 1, 4, 9, 16, 17, 25, 33, 36, 41, 49, 57.

For a modulus m which is the product of any number of powers of primes, the number of residues is obtained by taking the product of the number of residues for the separate powers of primes. Thus if $m = p_1^{\alpha_1}p_2^{\alpha_2}$, the solution of $X^2 \equiv D (\text{mod } m)$ is possible if and only if the separate congruences $X^2 \equiv D (\text{mod } p_1^{\alpha_1})$ and $X^2 \equiv D (\text{mod } p_2^{\alpha_2})$ are possible; and any solution of the first may be combined with any solution of the second to give a solution of the original congruence. Thus if $D \equiv \alpha (\text{mod } p_1^{\alpha_1})$ is such that the congruence $X^2 \equiv D (\text{mod } p_1^{\alpha_1})$ is solvable and $D \equiv \beta (\text{mod } p_2^{\alpha_2})$ such that the congruence $X^2 \equiv D (\text{mod } p_2^{\alpha_2})$ is solvable, then as the moduli are relatively prime to each other one and only one solution is possible of the two congruences, $D \equiv \alpha (\text{mod } p_1^{\alpha_1})$ and $D \equiv \beta (\text{mod } p_2^{\alpha_2})$ taken simultaneously and the resulting D makes $X^2 \equiv D (\text{mod } p_1^{\alpha_1} p_2^{\alpha_2})$ solvable. Thus the number of residues of the number 42 is equal to the product of the

number of residues of 2, 3 and 7. That is, $2 \cdot 2 \cdot 4$ or 16. The residues are in fact: 0, 1, 4, 7, 9, 15, 16, 18, 21, 22, 25, 28, 30, 36, 37, 39.

Consecutive Residues.—Certain interesting theorems[1] concerning the number of consecutive residues for a given prime number have been obtained for the current definition of a quadratic residue by M. Aladov[2] and also by M. von Sterneck.[3] The results of M. Aladov,—I have not seen the paper,—are as follows:

Let x = number of non-residues followed by a non-residue,
x' = number of non-residues followed by a residue,
y = number of residues followed by a non-residue,
y' = number of residues followed by a residue.

Then for p a prime of the form $4n + 1$ we have:

$$x = x' = y = \frac{p-1}{4}; \quad \text{and} \quad y' = \frac{p-5}{4}$$

and for p a prime of the form $4n + 3$ we have:

$$x = x' = y' = \frac{p-3}{4}, \quad \text{and} \quad y = \frac{p+1}{4}.$$

M. von Sterneck has extended these results to show that for every prime except 2, 3, 5, 7, 11, and 17, there is at least one group of four consecutive residues, or four consecutive non-residues.

M. Aladov's results are not difficult to obtain from a consideration of the congruence, $xy \equiv 1 \pmod{p}$. This congruence groups the $p - 1$ numbers, $1, 2, 3, 4, \cdots p - 1$, in pairs. For two values of x, namely, ± 1, the value of y is equal to x. For other values of x the value of y is different. There are then in all $(p + 1)/2$ pairs. Let x', y', be such a pair. Then there is another pair $(p - x')(p - y')$, and for our purpose these two pairs are not essentially distinct, as they furnish identical pairs of consecutive residues as follows: If we put $a + b \equiv x'$ and $a - b \equiv y'$ we obtain $a^2 - b^2 \equiv 1 \pmod{p}$, or a and b are consecutive residues. The pair $(p - x')(p - y')$ give the same pair of residues. The number of pairs of consecutive residues therefore would seem to be $(p + 1)/4$, and this is indeed the correct formula for p, a prime of the form $4n + 3$. For p a prime of the form $4n + 1$ the number of pairs will be odd and there will be one pair in which $x' = p - y'$, or in which the pair (x', y') is identical with the pair $(p - y', x')$. The number of distinct pairs of consecutive residues for such a prime is therefore $(p + 3)/4$. In these formulæ we have included the residue zero. Thus for the prime 11, we have the following pairs of values x, y and the corresponding values of a and b:

[1] These theorems have been proved by Jordan in his *Traite des Substitutions*, 1870, page 158 Professor Dickson has kindly called my attention to Jordan's proof, which is based on different principles from that given here.

[2] *Recueil Mathématique*, Société de Moscou, t. XVIII, 1895.

[3] *Ibid.*, t. XX, 1898.

$x, y.$	$p-x, p-y.$	Residues.
1, 1.	10, 10.	1, 0.
2, 6.	9, 5.	5, 4.
3, 4.	8, 7.	4, 3.

There are thus three consecutive pairs of residues for the prime 11. For the prime 17, we have the following pairs:

$x, y.$	$p-x, p-y.$	Residues.
1, 1.	16, 16.	1, 0.
2, 9.	15, 8.	9, 8.
3, 6.	14, 11.	16, 15.
4, 13.	13, 4.	17, 16.
5, 7.	12, 10.	2, 1.

Aladov's formula would give only three pairs because he does not admit the residue 0. This drops out the first and fourth pair.

The rest of M. Aladov's results follow without much difficulty. Thus for a prime of the form $4n + 1$, if we denote a residue by R, and a non-residue by N, our formula for the number of sequences RR is $(p + 3)/4$. For the sequence NN we may start from the congruence $xy \equiv N(\text{mod } p)$ and by an exactly similar line of reasoning derive the formula $(p - 1)/4$ for the number of pairs of residues differing by a given non-residue N. Let R' and R'' be two such, so that $R' - R'' \equiv N(\text{mod } p)$. Multiply now this congruence through by the non-residue N' which is such that $NN' \equiv 1(\text{mod } p)$ and we obtain a pair of non-residues differing by unity. For the sequences NR and RN we may see that they must be equal in number, for since -1 is a residue of primes of the form $4n + 1$ the sequence RN involves the sequence $-R, -N$, which when written $p - N, p - R$ is seen to be a sequence NR. Now the total number of sequences in the series of numbers $0, 1, 2, 3, 4, \cdots p - 1, p$ is equal to p. Of these there are $(p + 3)/4$ sequences RR, and $(p - 1)/4$, sequences NN. The remaining $(p - 1)/2$ sequences are equally divided among the sequences NR and RN, and are therefore $(p - 1)/4$ in number. With the notation used in stating M. Aladov's results we have, including the residue zero,

$$x = x' = y = \frac{p-1}{4}; \quad \text{and} \quad y' = \frac{p+3}{4}.$$

The case where p is of the form $4n + 3$ may be discussed in the same way,

$$x' = y' = y = \frac{p+1}{4}, \quad \text{and} \quad x = \frac{p-3}{4}.$$

I do not know whether M. Aladov has extended these results to apply to composite moduli or not. This we will do, and first we take the case where the modulus is a power of an odd prime p. We shall show how from a pair of consecutive residues for the modulus p^a we may derive p pairs of consecutive residues for the modulus p^{a+1}, unless one of the pair of consecutive residues for p^a is congruent to zero mod p^a.

Let $x_1^2 - y_1^2 \equiv 1 \pmod{p^\alpha}$ yield a pair of consecutive residues. Then $(x_1 + kp^\alpha)^2 - (y_1 + lp^\alpha)^2 \equiv 1 \pmod{p^\alpha}$ will yield the same pair for all values of k and 1. Multiply out and put $x_1^2 - y_1^2 - 1 = mp^\alpha$, then

$$mp^\alpha + 2(kx_1 - ly_1)p^\alpha + (k^2 - l^2)p^{2\alpha} \equiv 0 \pmod{p^\alpha}.$$

The last term on the left is congruent to zero mod $p^{\alpha+1}$ if α is greater than unity. The other terms will also be divisible by $p^{\alpha+1}$ if

$$m + 2(kx_1 - ly_1) \equiv 0 \pmod{p}.$$

In this congruence m, x_1, and y_1 are known and k and l are unknown. It may be shown that a congruence of the form $ax + by + c \equiv 0 \pmod{p}$ has exactly p roots, unless a and b are divisible by p, and c is not. We defer the proof of this theorem and note that if $y_1 \equiv 0 \pmod{p^\alpha}$ then the congruence $m + 2kx_1 \equiv 0 \pmod{p}$ yields only one effective pair, for no matter what the value of 1, the expression $(y_1 + lp^\alpha)^2$ will be divisible by $p^{\alpha+1}$ for α greater than one. Thus a pair of consecutive residues for the modulus p^α yields in general p consecutive residues for the modulus $p^{\alpha+1}$ except the consecutive pair (1, 0) which yields the one pair (1, 0). Also if p is of the form $4n + 1$ then a pair $(0, -1)$ is obtainable which likewise yields the single pair $(0, -1)$ for the modulus $p^{\alpha+1}$. The theorem is therefore proved.

The theorem regarding the number of solutions of the congruence $ax + by + c \equiv 0 \pmod{p}$ is a special case of the more general theorem:

The congruence $ax + by + c \equiv 0 \pmod{m}$ has $m\delta$ solutions, or none at all according as δ, the greatest common divisor of a, b and m, does or does not divide c.

The congruence clearly has no solutions when δ does not divide c. Take first the case when δ is unity, and let δ' be the greatest common divisor of a and m. Then from the well-known theory of the congruence $ax + b \equiv 0 \pmod{m}$, it is seen that there will be δ' values of x for every value of y satisfying the congruence $by + c \equiv 0 \pmod{\delta'}$. Now b is prime to δ' and therefore this last congruence has one and only one root β, say. The m/δ' numbers less than or equal to m and congruent to $\beta \pmod{\delta'}$ will serve as values of y, each of which will furnish δ' corresponding values of x. Other values of y will give no values of x at all. The total number of solutions in this case $m/\delta' \cdot \delta'$, or m. If now δ is not unity, we may divide both sides of the congruence through by δ and get the congruence $(a/\delta)x + (b/\delta)y + (c/\delta) \equiv 0 \pmod{(m/\delta)}$, which has by the above discussion, m/δ solutions. Let (α, β) be one of these. Then in place of α we may take any one of the δ numbers congruent to $\alpha \bmod (m/\delta)$ which are less than or equal to m. Similarly for β. The total number of solutions is therefore $(m/\delta) \cdot \delta \cdot \delta$, or $m\delta$, which proves the theorem. A similar line of reasoning will show that the number of solutions of the congruence $ax + by + cz + d \equiv 0 \pmod{m}$, is $m^2\delta$, or zero, according as δ, the greatest common divisor of a, b, c, and m does or does not divide d. Also in general, by an easy induction, we may establish that the number of solutions of the congruence $a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + \cdots a_nx_n + a_{n+1} \equiv 0 \pmod{m}$ is $m^{n-1}\delta$, or zero,

according as δ, the greatest common divisor of $a_1, a_2, a_3, \cdots a_n$ and m does or does not divide a_{n+1}. These theorems are, of course, special cases of the general problem of simultaneous linear congruences discussed by H. J. S. Smith (*Works*, Vol. II, p. 367).

We can now write down formulæ for the number of consecutive residues for a modulus which is the power of any odd prime p. We have seen that the number of consecutives for a prime of the form $4n + 1$ is $(p + 3)/4$, and leaving out the two sequences $(0, 1)$ and $(-1, 0)$ there remain $\{(p + 3)/4\} - 2$ ordinary sequences. For the modulus p^2 this must be multiplied by p and the two end sequences $(0, 1)$ and $(-1, 0)$ added, which gives for the modulus p^2 the total number of consecutive residues as $\{(p - 5)/4\}p + 2$. In general, for the power p^α the number of consecutive residues will be $\{(p - 5)/4\}p^{\alpha-1} + 2$. The formula is wrong for the prime 5, since in the case of that prime $(p + 3)/4$ is 2, and rejecting the two end consecutives would leave zero. The formula would always give the number as 2. This is correct for α equal to 1, or 2, but for α greater than 2 the correct formula is $4 \cdot 5^{\alpha-3} + 2$.

The argument is easily made also for p of the form $4n - 1$ and the formula is $\{(p - 3)/4\}p^{\alpha-1} + 1$, for the number of consecutive residues for the modulus p^α. The prime 3 is an exception. For α equal to 1 or 2 the number is 1. For α greater than 2 the number is $3^{\alpha-3} + 1$.

For a modulus which is a power of 2 the formula reduces to the greatest integer in $(2^{\alpha-5} + 5)/3$, for 2^α, where α is greater than 4. For α less than 4 the number of sequences is 1.

For the general composite modulus it is now possible to compute the number of consecutive residues. In fact the number of such residues for the product of two relatively prime numbers is equal to the product of the numbers for the two factors. Suppose that the two factors are p and q, and that we have found for each a pair of consecutive residues, so that

$$P_1 - P_2 \equiv 1 (\text{mod } p)$$

and

$$Q_1 - Q_2 \equiv 1 (\text{mod } q)$$

and that these come from the squares,

$$x_1^2 - y_1^2 \equiv 1 (\text{mod } p)$$

and

$$x_2^2 - y_2^2 \equiv 1 (\text{mod } q);$$

determine now k and l to satisfy the congruences:

$$x_1 + kp \equiv x_2 (\text{mod } q),$$

$$y_1 + lp \equiv y_2 (\text{mod } q);$$

p being prime to q these will have one and only one solution each. Thus the number of consecutive residues for the modulus pq is at least as great as the

product of the number of those for the modulus p by that for the modulus q. But since a residue of pq must necessarily be a residue of p and of q separately every pair of consecutive residues for pq will also be a pair of consecutive residues for p and q.

As an illustration of the method of finding consecutive residues for a composite modulus take the modulus $253 = 11.23$. For the modulus 11 we have the consecutive residues 3, 4 arising from 5^2 and 2^2. For the modulus 23 we have the residues 1, 2 arising from 1^2 and 5^2. The congruences $2 + 11k \equiv 5 (\text{mod } 23)$ and $5 + 11 \cdot l \equiv 1 (\text{mod } 23)$ give $k \equiv 17$, and $l \equiv 8 (\text{mod } 23)$. Then $2 + 187$, or 189, and $5 + 88$ or 93 must furnish a pair of consecutive residues for 253. It is found that $189^2 \equiv 48$ and $93^2 \equiv 47$. Since further there are 3 consecutive residues for the modulus 11, and 6 for the modulus 23 there will be 18 for the modulus 253.

In conclusion, a word should be said as to the determination of the possibility of the congruence $x^2 \equiv D (\text{mod } m)$ where D is not restricted to be prime to m. In the first place, it is necessary to consider only the case where the modulus is a power of a prime. For if x can be found such that $x^2 - D$ is divisible by pq, where p and q are relatively prime, then $x^2 - D$ will be divisible by p and q, and conversely. Consider then the modulus p^α; and let $D = Ap^\lambda$ where A is prime to p.

If λ is greater than α the congruence will have the root $x \equiv 0$.

I. Suppose that λ is less than α, and suppose first that A is a residue p of and write $A \equiv y^2 (\text{mod } p^\alpha)$. Then if λ is even the congruence is possible and has the root $x \equiv \pm yp^{\lambda/2}$.

II. If A is a residue of p and λ is odd the congruence has no roots. For writing $x^2 \equiv Ap^\lambda + Mp^\alpha$ then x contains p^λ as a factor. It must then contain another factor p. But the right side can contain no such factor.

III. If A is a non-residue of p and λ is even the congruence is impossible. For dividing out p^λ we would have the impossible congruence

$$x'^2 \equiv A (\text{mod } p^{\alpha-2}).$$

IV. If A is a non-residue, and λ is odd then Ap^λ is a non-residue. Proof as in case II. In general, then Ap^λ is a residue of p^α when λ is greater than or equal to α and when λ is less than α and even and A a residue of p.

THE GENERAL SOLUTION OF A CLASS OF INFINITE SYSTEMS OF EQUATIONS IN AN INFINITE NUMBER OF VARIABLES.

By THOMAS. E. MASON, Indiana University.

The problem of this paper is to find the general solution of the system of equations

$$\sum_{j=0}^{\infty} a_{ij} u_j = c_i, \quad i = 0, 1, 2, 3, \cdots, \tag{1}$$

where the coefficients a_{ij} are polynomials in i, of the form

$$a_{ij} = \alpha_j^{(0)} + \alpha_j^{(1)} i + \alpha_j^{(2)} i^2 + \cdots + \alpha_j^{(n)} i^n.$$

The system can be expressed in the form

$$(2) \quad \sum_{j=0}^{\infty} \alpha_j^{(0)} u_j + i \sum_{j=0}^{\infty} \alpha_j^{(1)} u_j + i^2 \sum_{j=0}^{\infty} \alpha_j^{(2)} u_j + \cdots + i^n \sum_{j=0}^{\infty} \alpha_j^{(n)} u_j = c_i, \quad i = 0, 1, 2, \cdots.$$

A necessary and sufficient condition that the general solution of (2) shall be the general solution of (1) is that for every solution of (1) each of the infinite series indicated by the summations in (2) shall converge. This condition will be shown to be fulfilled and the system will be studied in the form (2).

When $i = 0$ the infinite series in the first term of (2) converges[1] since it is the first equation of (1). Now add the negative of that series to (1) and the result can be written in the form

$$(3) \quad \sum_{j=0}^{\infty} (\alpha_j^{(1)} i + \alpha_j^{(2)} i^2 + \cdots + \alpha_j^{(n)} i^n) u_j = k_i, \quad i = 0, 1, 2, \cdots.$$

If any n consecutive equations of (3) are multiplied, the first by m_1, the second by m_2, $\cdots$, the nth by m_n, and the products added the result is of the form

$$\sum_{j=0}^{\infty} \{[m_1 i + m_2(i+1) + \cdots + m_n(i+n-1)]\alpha_j^{(1)} + [m_1 i^2 + m_2(i+1)^2 + \cdots + m_n(i+n-1)^2]\alpha_j^{(2)} + \cdots + [m_1 i^n + m_2(i+1)^n + \cdots + m_n(i+n-1)^n]\alpha_j^{(n)}\} u_j = k_i'.$$

Now let t be any integer of the set $1, 2, 3, \cdots, n$. Then for each value of i the m's can be chosen in such way as to make the coefficient of $\alpha_j^{(t)}$ equal to 1 and the coefficients of $\alpha_j^{(k)}$ equal to 0, when $k \neq t$. That the m's can be so chosen is evident from the fact that they are thus restricted to satisfy n non-homogeneous equations in n unknowns, the determinant of the system being different from zero. This would give

$$\sum_{j=0}^{\infty} \alpha_j^{(t)} u_j = k_t'', \quad t = 1, 2, \cdots, n,$$

that is, each of the infinite series of (2) converges for every solution of (1). Hence the general solution of (2) is the general solution of (1) and vice versa.

Write

$$(4) \quad \sum_{j=0}^{\infty} \alpha_j^{(t)} u_j = B_t, \quad t = 0, 1, 2, \cdots, n;$$

then (2) can be written

$$(5) \quad B_0 + iB_1 + i^2 B_2 + \cdots + i^n B_n = c_i, \quad i = 0, 1, 2, \cdots.$$

Difference this equation $n + 1$ times with respect to i and the result is

[1] Only such values of u_j are called a solution as make every first member of (1) convergent.

(6) $$\Delta^{n+1}c_i = 0,$$

that is,

$$c_{i+n+1} - (n+1)c_{i+n} + \frac{(n+1)n}{2!}c_{i+n-1} - \cdots + (-1)^{n+1}c_i = 0.$$

This is a necessary condition on the c's that equations (2) shall be consistent. The same condition on the c's can be obtained by taking consecutive values of i and eliminating the B's. We suppose that the c's satisfy this condition.

If $n+1$ consecutive values of i are taken in (5) the B's can be found in terms of the c's, since the determinant of the $n+1$ equations is different from zero. If these values of B_t are substituted in (4) the problem is reduced to solving the finite set of equations in an infinite number of variables:

(7) $$\sum_{j=0}^{\infty}\alpha_j^{(t)}u_j = B_t, \quad t = 0, 1, 2, \cdots, n.$$

If possible select $n+1$ of the u's such that the determinant of their coefficients is different from zero. Transpose to the second member of the equations the remaining u's. These can be given arbitrary values, provided that the second member of each equation converges. Then the remaining $n+1$ u's can be found by the Cramer method. The solution thus obtained has an infinite number of arbitrary elements. Obviously it is the general solution.

If no $(n+1)$th order determinant, not zero, exists in the first member of (7) it will be shown below that the equations in the system (7) are linearly dependent. If the equations are linearly dependent and are consistent there will be conditions on the B's like

$$\sum_{t=0}^{n} b_t B_t = 0,$$

where the b's are constants. The number of such conditions will depend on the number of equations which are dependent on the others. Since the B's are expressed in terms of the c's these are additional conditions which must be fulfilled by the c's.

To show that if all the $(n+1)$th order determinants of the coefficients in (7) are zero the equations are linearly dependent, it will be shown that if they are linearly independent there is at least one $(n+1)$th order determinant different from zero.

Set up the matrix of the coefficients of (7)

$$\begin{Vmatrix} \alpha_0^{(0)} & \alpha_1^{(0)} & \alpha_2^{(0)} & \alpha_3^{(0)} & \cdots \\ \alpha_0^{(1)} & \alpha_1^{(1)} & \alpha_2^{(1)} & \alpha_3^{(1)} & \cdots \\ \alpha_0^{(2)} & \alpha_1^{(2)} & \alpha_2^{(2)} & \alpha_3^{(2)} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha_0^{(n-1)} & \alpha_1^{(n-1)} & \alpha_2^{(n-1)} & \alpha_3^{(n-1)} & \cdots \\ \alpha_0^{(n)} & \alpha_1^{(n)} & \alpha_2^{(n)} & \alpha_3^{(n)} & \cdots \end{Vmatrix}.$$

The equations being assumed linearly independent, no row has each term zero, nor can any row be made to have each term zero by addition of multiples of other rows. If $\alpha_0^{(0)} = 0$ then we can move to the position of first column a column where the term in the first row is different from zero since not all the terms of any row are zero. Then by addition of multiples of this row all but the first term of the first column can be made zero. If $\alpha_1^{(1)} = 0$ then some column following has the term in the second row different from zero and it can be brought to occupy the position of second column. As before all the terms of this column below the second can be made zero by addition of multiples of the second row. Proceeding in this way a new matrix is obtained the first $(n + 1)$th order determinant of which will have all the terms below the principal diagonal equal to zero and each term of that diagonal different from zero. The determinant of the original matrix composed of those $n + 1$ columns which form the first $(n + 1)$th order determinant of the transformed matrix, is obviously not zero. Hence if the equations are linearly independent there will be at least one $(n + 1)$th order determinant different from zero, and hence if every $(n + 1)$th order determinant of the coefficients in (7) is zero the equations are linearly dependent.

In the case of linear dependence the equations which are dependent on others can be omitted and the general solution can be found from the linearly independent equations. This can be done as above by making arbitrary, with restriction as to convergence, all the u's except as many as there are equations and solving for these by the ordinary method.

PRECISE MEASUREMENTS WITH A STEEL TAPE OR WIRE.

By GEORGE R. DEAN, Rolla, Mo.

In the measurement of horizontal distances with a steel tape or wire in cases where all attainable accuracy is required, there will be considerable calculation avoided if the engineer has the means of knowing how to adjust the tension so that the elongation due to tension may balance the correction for sag or droop. Under ordinary conditions the correction for temperature is negligible, and when not negligible is easily applied and need not be discussed here.

We will derive a formula for the sag correction and the stretch separately. Then by equating these corrections, derive a formula for the tension in terms of the weight, cross-section and modulus of elasticity of the tape or wire.

Correction for Sag.—This is usually derived by the aid of the calculus in text-books on mechanics, but the calculus is unnecessary for this purpose, if we assume that the curve is the arc of a circle. The approximate formula derived in this way is the same as that obtained by integration when the curve is taken as a catenary or a parabola.

Let R = radius of circle,
l = length of tape or wire in inches,
α = number of radians in half the angle at center,
h = horizontal distance in inches,
δ = sag in inches.

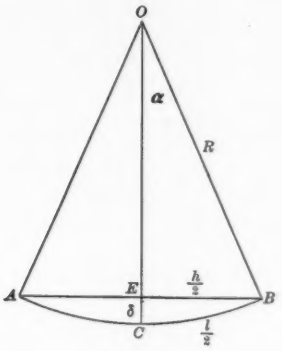

FIG. 1.

In Fig. 1,

$$OA = OB = OC = R,$$

$$\angle COB = \alpha, \quad \text{and} \quad EC = \delta.$$

$$AB = h, \quad ACB = l.$$

Then

$$l = 2R\alpha, \tag{1}$$

$$h = 2R \sin \alpha, \tag{2}$$

$$\delta = R(1 - \cos \alpha). \tag{3}$$

Since α is in practice a very small angle, we may write as approximations,

$$\sin \alpha = \alpha - \frac{\alpha^3}{6}, \quad \text{and} \quad \cos \alpha = 1 - \frac{\alpha^2}{2},$$

using the first two terms of the sine and cosine series. Then our equations (1), (2), (3), become

$$l = 2R\alpha, \tag{4}$$

$$h = 2R\left(\alpha - \frac{\alpha^3}{6}\right), \tag{5}$$

$$4\delta = 2R\alpha^2. \tag{6}$$

Dividing (6) by (4),

$$\alpha = \frac{4\delta}{l}. \tag{7}$$

Dividing (5) by (4),

$$1 - \frac{\alpha^2}{6} = \frac{h}{l}. \tag{8}$$

From (8),

$$h = l - \frac{l\alpha^2}{6}.$$

Substituting value of α from (7)

$$h = l - \frac{8\delta^2}{3l}. \tag{9}$$

Then the correction for sag is $8\delta^2/3l$.

Correction for Tension.—Let T be the pull at each end, w the weight of tape or wire per unit length, a the area of cross-section in square inches, E the modulus of elasticity of the material, θ the angle between the direction of the pull and the horizontal. The smaller the sag the more nearly will CF be equal to CE (Fig. 2).

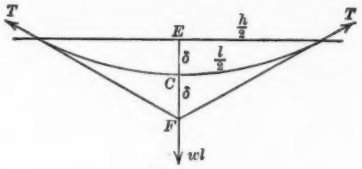

FIG. 2.

The forces T, T and wl are in equilibrium. The vertical component of each pull is $T \sin \theta$. Then we have

$$2T \sin \theta = wl. \tag{10}$$

Now

$$\sin \theta = \frac{\frac{2\delta}{2}}{l} = \frac{4\delta}{l}, \text{ approximately.}$$

Then

$$2T\left(\frac{4\delta}{l}\right) = wl,$$

or

$$T = \frac{wl^2}{8\delta}. \tag{11}$$

If x denote the elongation,

$$x : l = \frac{T}{a} : E,$$

or

$$x = \frac{lT}{aE}. \tag{12}$$

Equating this to the correction for sag,

$$\frac{lT}{aE} = \frac{8\delta^2}{3l}. \tag{13}$$

From (11),

$$\delta = \frac{wl^2}{8T}.$$

Substituting in (13),

$$\frac{lT}{aE} = \frac{8w^2l^4}{64T^2 \cdot 3l} = \frac{8w^2l^4}{192T^2l}.$$

Solving for T,

$$T^3 = \frac{aEw^2l^2}{24}, \tag{14}$$

or

$$T = \sqrt[3]{\frac{aEw^2l^2}{24}},$$

and since $wl = W$ the weight of tape,

$$T = \sqrt[3]{\frac{aEW^2}{24}}. \tag{15}$$

Numerical Example.—If the weight of tape is 5 pounds, the modulus of elasticity 30,000,000 pounds per square inch, and the area of cross-section .015 square inch,

$$T = \sqrt[3]{\frac{.015 \times 30{,}000{,}000 \times 25}{24}} = 77.5 \text{ pounds.}$$

and

$$\delta = \frac{Wl}{8T} = \frac{5 \times 5}{8 \times 77.5 \times .015 \times 0.3} = \frac{25}{77.5 \times .036} = 8.9 \text{ inches.}$$

Here

$$l = \frac{5}{.015 \times 0.3} = 1{,}111.1 \text{ inches} = 92.5 \text{ feet.}$$

BOOK REVIEWS.

W. H. BUSSEY, Chairman of the Committee.

Practical Geometry and Graphics. A text book for students in technical and trade schools, evening classes, and for engineers, artisans, draughtsmen, architects, etc. By E. L. BATES and F. CHARLESWORTH. Van Nostrand, New York, 1912. viii + 621 pages. $2.00.

Practical Mathematics. By E. L. BATES and F. CHARLESWORTH. Van Nostrand, New York, 1912. viii + 513 pages. $1.50.

These two texts, which have been written in part to prepare for the examinations of the London Board of Education, are essentially what they claim to be, that is for practical men. In fact they almost take the form of an engineering pocket book. The ground covered is enormous, the proofs whenever given are brief and frequently of an experimental nature, such as would appeal to good

mechanics with little mathematical training. Both texts are very well illustrated, well written, and published in an attractive form, with an immense number of examples which make them very convenient for students working alone.

The two books cover a great deal of common ground. The first is written more especially for draughtsmen and for such practical work as requires graphics. It deals with conics, graphostatics and descriptive geometry. The second book has a broader scope and is more especially for mechanics and designers. It contains algebra, geometry, trigonometry, vectors, and calculus. Both books are to be recommended to the class of students which they aim to reach, and also to more advanced readers for the numerous and well chosen practical examples which they contain.

S. LEFSCHETZ.

Life Assurance Primer. A text book dealing with the practice and mathematics of life insurance, for advanced schools, colleges and universities. By HENRY MOIR. Third edition, revised and enlarged. The Spectator Company, New York, 1912. vii + 230 pages. $2.00.

In recent years, there has been a tendency both in Europe and America to extend university education to include something of the principles of insurance. This work in insurance has often taken the form of a treatment of the economics of insurance; but it has also been recognized that any substantial development of the elementary principles of insurance very naturally takes a mathematical form. The present book is found to be very useful as a beginning text for teaching the elements of this subject. The reviewer has used the second edition, and is at present using the third edition in a class of twenty students of junior and senior rank, and is prepared to say that he finds the book teachable. In this last edition the material has been thoroughly revised, and much improved for purposes of university instruction. A new chapter has been added dealing with the organization and management of a life company. One of the new features is the introduction of questions, exercises, and problems at the end of each chapter. This addition will surely commend itself to teachers of the subject. The book serves well as a text for a beginning course of approximately two hours per week for a semester; and, although the reading of the book requires hardly any more mathematics than the algebra usually included in a freshman course, it is not too easy for the beginner, as a comprehension of the business situations involved requires considerable knowledge, and the expression of such situations in mathematical form requires a good deal of thought.

H. L. RIETZ.

Source Book of Problems for Geometry. By MABEL SYKES, with the coöperation of H. E. SLAUGHT and N. J. LENNES. Allyn and Bacon, Boston, 1912. viii + 372 pages.

The present volume is a welcome contribution to the endeavor to make the mathematical work in our schools more practical and tangible. The belief

that mathematics is an excellent discipline has for many years removed the mathematics of the secondary schools farther and farther from the daily life and experience of the pupils. The text-books have emphasized the logical side, and have contained a large number of exercises and problems for drill and a few problems in applied mathematics which are for the most part spurious. We are, however, coming to realize in a larger measure that the great majority of boys and girls finish their education in the grammar school or the high school, and that the algebra and the geometry of the schools should prepare pupils as far as possible to do well the work that falls to them after leaving school.

In courses in architecture and design this *Source Book of Problems* meets the demand that a text-book shall have continuous and practical connection with working conditions. All of the problems have to do with real things, and are solved by the practical application of geometrical principles. The titles of the six chapters show the practical character of the book. The titles are: (1) Tile designs; (2) Parquet floor designs; (3) Miscellaneous industries; (4) Gothic tracery: Forms in circles; (5) Gothic tracery: Pointed forms; (6) Trusses and arches. The index of theorems and problems will aid the teacher in selecting the material so as to keep the logical continuity intact. In solving the problems the principles of arithmetic, algebra, and geometry are combined to such an extent that a thorough review of the former subjects is given, while the use of algebraic notation and methods makes the solutions much simpler and easier.

As a supplementary book in the high school course in geometry this text will, in the writer's opinion, prove of great value. Geometrical forms occur so frequently in tiles, mosaics, needlework, jewelry, iron grills, steel ceilings, tracery of windows and other architectural forms that a study of these forms will add greatly to the interest of geometry. Moreover it will be a pleasure to recognize known geometrical forms in architectural details which meet the eyes daily but have failed to attract attention.

The historical accounts of the various designs and the pictures of windows and other architectural details of famous buildings are of general educational value. There are over 1,800 exercises, and many of these are general problems from which it is possible to form any number of numerical problems. The drawings and illustrations number more than 450; they are well drawn and reproduced on excellent paper. The extensive bibliography and list of commercial catalogues enables the teacher to secure additional material if desired. The author, editors and publishers are to be congratulated on the appearance of this book.

H. E. Cobb.

PROBLEMS AND QUESTIONS.

B. F. FINKEL, Chairman of the Committee.

The solutions of problems and the proposal of new problems will be continued in the June issue.

NOTES AND NEWS.

FLORIAN CAJORI, Chairman of the Committee.

The answer book to Davis's Calculus is not expected to be published until next fall.

A new "College Algebra" by W. Benjamin Fite, Professor of Mathematics in Columbia University, has just been published by D. C. Heath and Company.

The meeting of the Association of Ohio Teachers of Mathematics and Science which was to have been held at Columbus at the end of March, was postponed indefinitely on account of the floods over Ohio.

Dr. Willy Wien, professor of physics in the University of Würzburg, delivered in April at Columbia University six lectures on "Recent Problems of Theoretical Physics."

It is proposed to hold an international congress of education in connection with the Panama-Pacific International Exposition, which is to take place in San Francisco in 1915. Efforts are being made to hold a large number of other scientific meetings in connection with this exposition.

M. d'Ocagne, professor at the Paris Polytechnic School, was elected president of the "Commission du Répertoire" to succeed M. Poincaré. This commission is publishing an extensive catalogue, in the form of small cards, of the mathematical literature up to 1900. These cards are sold by the well-known French publishers Gauthier-Villars, Paris, France.

The Smithsonian Institution of Washington obtained permission to include in the "Annual Report of the Board of Regents to Congress" the paper by Professor G. A. Miller, entitled *Some thoughts on modern mathematical research*, which appeared in Science, June 7, 1912.

During the latter part of April, the National Academy of Sciences celebrated its fiftieth anniversary at the Smithsonian Institution of Washington. A number of distinguished scientists were invited as guests. Among the ten new members elected at this meeting was Dr. L. E. Dickson, professor of mathematics at the University of Chicago.

The list of papers presented at the April meeting of the California section of the American Mathematical Society was as follows: "A set of postulates for the algebra of positive rational numbers with zero," by Mr. B. A. Bernstein; "On

the arithmetic value of quadratic forms," by Professor H. F. Blichfeldt; "The analytical geometry of functional space," by Dr. L. I. Neikirk; "Concerning the residues of certain sums of powers of integers to a prime modulus," by Professor T. M. Putnam; "A geometrical transformation, with some applications to certain systems of spheres," by Dr. H. W. Stager.

Mr. James S. Mikesh, instructor in mathematics at the University of Minnesota, has been granted a leave of absence for the year 1913–14. He will do graduate work at Harvard University where he has been appointed instructor in mathematics on part time for one year. Mr. Walter E. Anderson has been appointed an instructor in mathematics in the University of Minnesota for the year 1913–14 to take the place of Mr. Mikesh.

Mr. W. E. Heal, of Washington, D. C., calls attention to an error in the eleventh edition of the Encyclopædia Britannica, Vol. XIX., page 858, where it is stated, under the article on number, that "Kummer proved the very curious fact that p is regular if, and only if, it is not a factor of the denominators of the first $\frac{1}{2}(p-3)$ Bernoullian numbers." What Kummer really proved is, of course, that p is regular if, and only if, it is not a factor of the *numerator* of *any* of the first $\frac{1}{2}(p-3)$ Bernoullian numbers.

PROFESSOR H. WEBER, the author of the large algebra in three volumes, entitled *Lehrbuch der Algebra*, has recently published an abridged edition in one volume of 528 pages. The fifteen chapters bear the following headings: determinants, numbers and integral functions, symmetric functions, roots, cubic and biquadratic equations, Sturm's theorem, approximation of roots, groups, the Galois theory, cyclical equations, division of the circle, solution of the cyclical equation, algebraic solution of equations, numbers and functions of an algebraic realm, applications to cyclical realms. From these headings it appears clear that the work is not restricted to the most elementary parts of algebra, but that some of the more advanced subjects are included. The historical notes add greatly to the value of the work. A few of these seem inaccurate. For instance, on page 192 it is implied that the common symbol for quotient group is due to Hölder, but this symbol was used by Jordan at a much earlier date. On page 196 it is stated that Dedekind first divided a group into double co-sets in 1894. On the contrary it is well known that Frobenius developed this subject extensively in 1887. In the index on page 526 there appears "Normalleiter" instead of "Normalteiler."

The third volume of the *Taschenbuch für Mathematiker und Physiker* has recently been published by B. G. Teubner. This volume of 463 pages aims to serve as a convenient reference book for mathematicians and physicists. To enable the publishers to sell this edition at a low price the volume has been reduced in size to the extent of about 100 pages. Most of this reduction has been made in the parts relating to mathematics. The present volume still contains, however, a large amount of important mathematical information in a very compact and convenient form for the purpose of attaining a general idea of some

broad fields of modern knowledge. The new mathematical articles which are included in this third volume bear the following headings: Theory of aggregates, theory of groups and the Galois theory of equations, the last theorem of Fermat, integral equations and their applications, multiply valued functions and uniformisation, international commission on the teaching of mathematics, and analytical mechanics.

According to a circular of the *Encyclopédie des Sciences Mathématiques*, dated January, 1913, the seven tomes which have been planned are to contain 208 articles. The published fascicules of this work contain 34 articles, and 44 articles were in press at the time when this circular was issued. By comparing the present circular with the one issued about a year earlier, and inserted in the February, 1912, number of the *Bulletin of the American Mathematical Society*, it appears that a considerable number of changes have been made with respect to the collaborators. The list of collaborators of the German edition indicates that about ten names were replaced by others, while the main changes in the list of collaborators of the French edition are the addition of six new names and the dropping of Poincaré's name. The lists of collaborators include the following names of American mathematicians: Maxime Bôcher, Harvard University; E. W. Brown, Yale University; J. Harkness, McGill University; Kurt Laves, University of Chicago; G. A. Miller, University of Illinois; F. R. Moulton, University of Chicago; W. F. Osgood, Harvard University.

Plans for the Napier tercentenary celebration are described in *Nature* as follows: "The council of the Royal Society of Edinburgh, mindful of the greatness of the boon conferred on science by Napier's invention, convened a committee representative of some twenty societies, corporations, and institutions to discuss the proposal to hold a celebration in memory of the event. The universities and colleges of Scotland, the Faculty of Actuaries, the Edinburgh Mathematical Society, the Institute of Bankers, and other like bodies, also the Royal Society of London and the Royal Astronomical Society, were represented by delegates to the first meeting of the committee, which was held in the Royal Society Rooms, 22 George Street, Edinburgh, on Saturday, February 22. Mr. J. R. Findlay, one of the representatives of the Edinburgh Merchant Company, was voted to the chair. . . . An executive committee was nominated to carry into effect the following resolutions: That a congress be held in the summer of 1914, to be opened by a public reception and an address by an eminent man on some aspect of Napier's life and work; that, in response to an invitation from the directors of Merchiston Castle School, a garden-party be held in the grounds of Merchiston Castle; that papers be read on methods of calculation and of mathematical teaching; that exhibits be made of all kinds of calculating machines, of logarithmic and other mathematical books which are necessary for calculation, and of objects of historic interest associated with the name of Napier; that eminent mathematicians be invited from foreign countries to take part in the celebration; (and) that a memorial volume be published containing the more important of the addresses and communications.

6

THE

AMERICAN

MATHEMATICAL MONTHLY

VOLUME XX JUNE, 1913 NUMBER 6

INCENTIVES TO MATHEMATICAL ACTIVITY.

By H. E. SLAUGHT, University of Chicago.

Sources. During the past ten years there has been a marked activity among teachers of mathematics in this country, looking toward improvement in methods and the reconsideration of subject matter, especially with reference to selection and emphasis. In this activity we are by no means alone. In fact, there has probably been still greater readjustment on the other side of the water. Doubtless the so-called Perry movement in England may be considered as one of the chief awakening influences underlying our own activity. But Professor Moore's presidential address[1] before the American Mathematical Society in December, 1902, "On the Foundations of Mathematics," may have been the real source of inspiration in this country which led to the special period of activity beginning at about that time.

The International Commission. As a world movement, all the activities in the various civilized countries were finally centered in the International Commission on the Teaching of Mathematics appointed by the Fourth International Congress of Mathematicians at Rome in 1908, on the motion of Professor D. E. Smith, of Columbia University. For four years this Commission occupied itself with collecting and publishing the fullest possible information as to the present status of the teaching of mathematics in each of the countries represented, not making any attempt thus far to propose or discuss reforms of any kind. The first report of this commission was made at the Fifth International Congress[2] held in Cambridge, England, in August 1912, where twenty-seven countries were represented and one hundred and fifty printed reports were presented, leaving about fifty still to be completed. The work of the commission will be continued

[1] *Bulletin of the American Mathematical Society*, Vol. IX, May, 1903, pp. 402–424. This article contains numerous references to the literature on this subject.

[2] For a general report of this Congress see the *Bulletin of the American Mathematical Society*, Vol. XIX, December, 1912, January, 1913. For a special report on the pedagogical aspects of the work of this Congress see THE AMERICAN MATHEMATICAL MONTHLY, Vol. XIX, October, 1912.